MARS RECONNAISSANCE ORBITER (MRO) 2005 PROJECT

Project Safety Plan

JPL D-20329

April 12, 2001

Jet Propulsion Laboratory
California Institute of Technology

MARS RECONNAISSANCE ORBITER (MRO) 2005 PROJECT

Project Safety Plan (Draft)

Prepared By:

Kirk D. Barrow 4/17/2001

Kirk D. Barrow
Project Safety Engineer

Approved By:

Phillip R. Barela
Mission Assurance Manager

4/17/01

James E. Graf
Project Manager

April 2001

Jet Propulsion Laboratory
California Institute of Technology

Change Log:

Change Log:

All changes and revisions to this Safety Plan will be coordinated through the MRO-05 Project Office.

Date	Affected Pages	Comment
April 12, 2001	All	Original (Draft) Issue

FORWARD

In response to the recommendations by its advisory groups, NASA is currently undertaking a long-term systematic program of Mars exploration, the Mars Exploration Program (MEP). The overarching goal of the program is to answer the question *"did life ever exist on Mars?"* The scientific objectives established by the program to address this goal are to search for evidence of past or present life, to understand the climate and volatile history of Mars, to understand the surface and subsurface geology, and to assess the nature and inventory of resources on Mars in preparation for human exploration. The common thread that links these objectives is to understand the role of water.

The theme for the 2005 Orbiter, is to provide global access of Mars from a low altitude that will conduct Remote sensing science observation, conduct site characterization for future potential landers and provide a UHF telecom relay capability for follow-on missions.

This page intentionally left blank.

CONTENTS

FIGURES

This page intentionally left blank.

SECTION 1 GENERAL

1.0 PURPOSE

This Safety Plan set forth uniform requirements for safety management, safety design and operation safety to be practiced by all organizations involved with providing an Orbiter and ground support equipment associated with the Mars Reconnaissance Orbiter Project, hereinafter refereed to as the MRO-05. It fills the requirement for a project safety plan of JPL's D-560, NASA Prime Contract NAS7-1407 and the Range Safety requirement of EWR 127-1.

It is furnished as a basis from which MRO-05 Project Management can generate safety activities and/or plans which will assure an acceptable level of safety through interface evaluations, risk control, and reporting methods acceptable to the Project and its interfacing agencies. The total safety activity will assure that an acceptable risk level is achieved by the overall Project design and activities, and that the MRO-05 Project Manager can certify that the orbiter is safe to launch utilizing the NASA provided intermediate Class launch vehicle (e.g. Delta III/IV, Atlas III/V).

1.1 SCOPE

This plan shall apply to the orbiter (the orbiter is the composite of the engineering subsystem and the payload after integration), ground support equipment and launch services within the MRO-05 Project. Government-mandated occupational safety and health activities contribute to the overall effectiveness of this plan but are addressed in a separate plan. As such, the contacrtor shall be reponsible for the integrated engineering subsystem and the payload.

The payload will consists of the following:

(a) Science instruments. Final science instrument will be selected via the NASA HQ Announment of Opportunity process, which is not expected to be complete until late summer 2001.

(b) 2 engineering elements. First, an UHF communication and navigation package called Electra. Second, an optical navigation camera experiment

(c) 3 Government-Furnished Properties, namely a Small Deep Space Transponder (SDST), a Traveling Wave Tube (TWT), and a Command Decoding ASIC.

Therefore, the Payload provider is the organization(s) providing hardware/software as stated in (a), (b) and (c) above to the contractor for integration.

1.2 RELATIONSHIP WITH OTHER CONTRACTURAL REQUIREMENTS

Organizations (contractor & payload provider) with contracts with the MRO-05 Project shall also adhere to this safety plan. If any requirement in this plan conflict with those in an agreement or a contact document binding on the organization, the requirement in the contracts document shall prevail over those contain in this plan.

1.3 CONTRACTOR/PAYLOAD PROVIDER RESPONSIBILITIES

The Orbiter contractor and payload provider shall each submit a safety plan for MRO-05 Project approval and also be responsible for taking actions required to ensure safety of and in connection with their personnel, hardware and GSE in accordance with the requirements in this plan and the contact documents.

It is the policy of JPL and the MRO Project to ensure personnel safety and hardware in consonance with project achievement. All MRO Project personnel shall be responsible for performing their duties in a safe manner. The project will conform to all local, state and federal regulations regarding safety.

Safety risk shall be eliminated or minimized through the application of safety engineering and system safety principles.

Project Managers, engineers, designers and test personnel shall have a thorough knowledge of system safety practices and shall apply their knowledge to assure a safe and successful mission.

SECTION 2

APPLICABLE DOCUMENTS

The minimum safety related documents applicable to the MRO-05 Project are listed below: In addition, where required, NASA guidelines, JPL institutional polices and practices, and the Eastern Range requirements shall be implemented. Contractor best polices and practices that meet or exceed JPL requirements are encouraged to be used.

Number	Title
Air Force	
EWR-127-1	Eastern and Western Range Safety Requirements
JPL	
D-560-	JPL "Standard for Systems Safety"
D-20327	"MRO Project Mission Assurance Plan"
D-17868	Design, Verification/Validation and Operations Principle for Flight Systems
KSC	
KHB.1710.2D	"KSC Safety Practices Handbook"
NASA	
STD-8719.8	"Expendable Launch Vehicle Payload Safety Review Process"
NPG 8621.1	NASA Procedures and Guidelines for Mishap Reporting, Investigation and Record Keeping
NSS 1740.14	Guidelines and Assessment Procedures for Limiting Orbital Debris

This page intentionally left blank

SECTION 3

SYSTEM SAFETY PROGRAM

3.1 System Safety Organization and Responsibilities

The MRO-05 Project management organization is shown in Figure 1. The Project Safety Engineer reports directly to the Project Manager on safety matters concerning flight hardware, software, ground support equipment, facilities or personnel.

3.1.1 System Safety Responsibilities

3.1.1.1 Jet Propulsion Laboratory

The Jet Propulsion Laboratory is the cognizant agency for the entire MRO-05 Project. The safety responsibility of JPL is for insuring that all organizations involved with providing an orbiter and GSE adequately address all safety requirements and that the MRO-05 mission is completed in a safe fashion. In addition, the MRO-05 Project must comply with safety requirements which are established by both JPL and external organizations such as the Air Force, NASA Kennedy Space Center, EPA, DOT, etc.

Project Manager

The MRO-05 Project Manager is responsible for the total safety performance of the project and is responsible for certifying that the orbiter is safe to fly on the NASA provided intermediate class launch vehicle. The MRO-05 Project Manager implements the MRO-05 safety program, chairs the MRO-05 Safety Steering Committee (SSC), assures all hazards associated with the orbiter and operations are identified and eliminated (or controlled), assures all safety requirements are met (or waived by competent authority), assures all JPL standards (or equivalent) are observed.

Project Safety Engineer

The Project Safety Engineer is principal advisor to the Project Manager for safety matters, identifies and clarifies safety requirements for the MRO-05 Project, coordinates safety issues with interfacing organizations, verifies closure of SCC action items, and audits execution of this safety plan by the project. As such, he/she will be responsible for the following:

(a) Supervise the preparation of safety documentation.
(b) Review the Missile System Prelaunch Safety Package (MSPSP) that will be presented to the Safety Steering Committee, and approves the MSPS published by the contactor prior to submittal to the Eastern Range (Ref. Figure. 2).
(c) Assures appropriate hazard analyses, tests and inspection are completed.
(d) Obtains JPL technical concurrence with safety verification data.
(e) Informs MRO-05 personnel of safety requirements and hazards.

(f) Assures potential hazards have been identified in drawings, specifications, and procedures.
(g) Approving all hazardous and safety critical test plans and procedures.
(h) He will have insight into the safety integration of the Orbiter by the Contractor, and report the status of safety activities at reviews.

Safety Steering Committee

Safety aspects of the MRO-05 orbiter, it GSE, operations, and interfaces are evaluated at appropriate by a review panel, the MRO-05 Safety Steering Committee (SSC). Panel membership includes as a minimum the MRO-05 Project Project Manager, Project Safety Engineer, and members of the orbiter contractor SSC. Panel chairmanship is normally the MRO-05 Project Manager, who announces the remaining membership by memorandum. A recorder and other members may also be appointed. Duties of the SSC chairman and members are specified in JPL D-560. At certain review milestone, the SSC meets to review and approve the MSPSP. The SSC ensures that the analysis of hazards is adequate and level of assumed risk is acceptable. Changes to the safety data package directed by the SSC are incorporated into the MSPSP before it is submitted to the Eastern Range (ER). The SSC may meet at other times as required.

JPL is responsible for the integrated MRO-05 Orbiter and launch vehicle and will certify that the integrated MRO-05 Orbiter & LV is safe for flight.

Launch Vehicle

Safety responsibilities for the launch vehicle/upper stage reside with the intermediate class launch vehicle provider, as determined by the terms of their contract with NASA. The Launch Vehicle provider is responsible for the safety of the launch vehicle and for assuring that it is acceptably safe for flight.

Figure 1 MRO 2005 Project Organization Chart

(TBD)

Figure 2: System Safety Responsibilities
MRO 2005 Project

Function	Contractor	Payload Provider	JPL
	Orbiter	P/L	Project
Publish project safety plan			P
Publish Orbiter system safety plan	P		RA
Publish Payload safety plans		P	RA
Prepare and present Concept Briefing to ER	PT	R	RA
Tailor Range Safety requirements document (EWR-127-1)	J	J	J
Establish and distribute safety requirements	P	P	P
Attend & participate in major design reviews	P	P	PR
Co-ordinate and integrate safety efforts with: vendors, launch vehicle NASA center, launch vehicle supplier, KSC and AF	P		RA
Edit and publish a Missile System Pre-launch Safety Package (MSPSP)-At least two required: preliminary and final	PRAT	R	RA
Submit any safety waiver requests that may be required from KSC and AF	PRAT	R	P
Assure compliance with Dept. of Transportation requirements for shipment of hazardous materials. Prepare exemption requests as required	PT		RA
Submit Non-ionizing Use Requests and associated personnel Experience Summaries	PT		R
Accept the responsibility for environmental protection and function as the project Environmental Protection Officer while at KSC/CCAS	P		R
Submit Process Waste Questionnaires and Hazardous Materials Log to KSC	PT		R
Establish training and medical certification requirements with the Eastern Launch Site office	PT		R
Participate in pre-test and pre-operations safety surveys. Monitor testing activities to assure compliance with safety requirements	P	P	P
Establish residency at the launch site to monitor and coordinate efforts to insure safety during pre-launch processing	P		P
Review industry SAF-ALERTS for applicability to the project and distribute the information as appropriate	P	P	P
Review and approve hazardous procedures for pre-launch processing and submit to ER for approval	PRAT		RA
Provide a Launch Site Safety Plan to the launch site.	PRAT	R	RA
Review ECR's to determine safety impact	P		RA
Review P/FR's to ensure appropriate safety rating and corrective action	P	P	RA

LEGEND:
P-Primary responsibility to prepare or perform function
J-Joint responsibility to prepare or perform
R-Review data or document
A-Approve data or document
T-Formally transmit to appropriate organizations

3.1.1.2 Contractor's Safety Organization

It is the responsibility of the Orbiter Contractor Program Manager to obtain a proper safety plan from each subcontractor. To the maximum extent possible, existing organization plans

should be used. The Orbiter Contractor's Program Manager is also responsible for subcontractor safety evaluations, requirements, and controls. Responsibilities include activities such as furnishing safety requirements and interface information to the subcontractor and obtaining appropriate safety evaluations and reports from the subcontractor. The Orbiter Contractor safety engineer will review, comment on, and finally approve all of their contractually required safety plans for all subsystem contractors when their contents are considered acceptable.

The Orbiter Contractor Program Manager must also assure that their contract specifies the safety requirements for equipment safety verification. Verification of safety certification must be furnished to the MRO-05 Project Safety Engineer to assure that sufficient information is available to the MRO-05 Project Manager for the KSC/CCAFS safety evaluation.

Safety requirements must be met on a schedule that is consistent with the overall MRO-05 Project schedule in order to meet its safety obligations with the Eastern Range (ER). Scheduled milestones such as safety reviews, data submittal, and verification procedures should be a part of safety planning in each area.

The Contractor's Systems Safety Organization is responsible for the following:

a) Design, development, fabrication and test of the engineering subsystems.

b) Integration of each payload.

c) Assembly and test of the orbiter.

d) Shipment to KSC and all pre-launch operations.

e) Design and manufacture of all engineering subsystem ground support equipment (GSE).

f) Generate the orbiter MSPSP and transmittal to ER.

g) Interfacing with all non-JPL organizations on any issues involving personnel and equipment safety.

3.1.1.3 Payload Provider Safety Orginazation

It is the responsibility of each Payload Provider Program Manager to obtain a proper safety plan from each subcontractor. To the maximum extent possible, existing organization plans should be used. The Payload Provider Program Manager is also responsible for subcontractor safety evaluations, requirements, and controls. Responsibilities include activities such as furnishing safety requirements and interface information to the subcontractor and obtaining appropriate safety evaluations and reports from the

subcontractor. The Payload Provider safety engineer will review, comment on, and finally approve all of their contractually required safety plans for all subsystem contractors when their contents are considered acceptable.

The Payload Provider Program Manager must also assure that their contract specifies the safety requirements for equipment safety verification. Verification of safety certification must be furnished to the MRO-05 Project Safety Engineer to assure that sufficient information is available to the MRO-05 Project Manager for the KSC/CCAFS safety evaluation.

Safety requirements must be met on a schedule that is consistent with the overall MRO-05 Project schedule in order to meet its safety obligations with the Eastern Range (ER). Scheduled milestones such as safety reviews, data submittal, and verification procedures should be a part of safety planning in each area.

The Payload Provider Systems Safety Organization is responsible for the following:

h) Design, development, fabrication and test of the payload.

i) Shipment to the contractor for integration.

j) Design and manufacture of all payload ground support equipment (GSE).

k) Provide inputs to the orbiter MSPSP.

l) Interfacing with all non-JPL organizations on any issues involving personnel and equipment safety.

Each payload provider is responsible for the design safety performance of his hardware. The responsibility for personnel safety, and safety of instrument test and operations shall remain with the payload provider until the instrument is delivered to the Orbiter Contractor. At that point the Orbiter Contractor shall assume responsibility for the safety of the instrument and any ancillary equipment (GSE) throughout integration with the Orbiter and all subsequent test and operations up to and including launch.

3.1.2 Integration and Coordination of Safety

An overview of the MSPSP integration activities, is provided in Figure 3. Since the MRO-05 Project encourages the empowerment of all personnel on the team, each orgaination cognizant engineer (Cog.E) will determine potential hazards associated with their subsystem design and operation. They will also insure that the information provided is accurate for inclusion into the Missile Systems Prelaunch Safety Package (MSPSP). Figure 3 shows the MSPSP generation.

The Orbiter Contractor’s System Safety Engineer will integrate the inputs into the MSPSP and coordinate the review of the package with the ER. JPL will have final approval of the MSPSP prior to submitting to the ER.

3.1.3 Outside Safety Activities

The following working groups and review panels work in coordination to assure mission safety:

a) High Performance Work Team (HPWT)

As specified by EWR-127-1, a High Performance Work Team (HPWT) shall be formed to perform tailoring of the EWR 127-1 during Technical Interchange Meetings (TIMs).

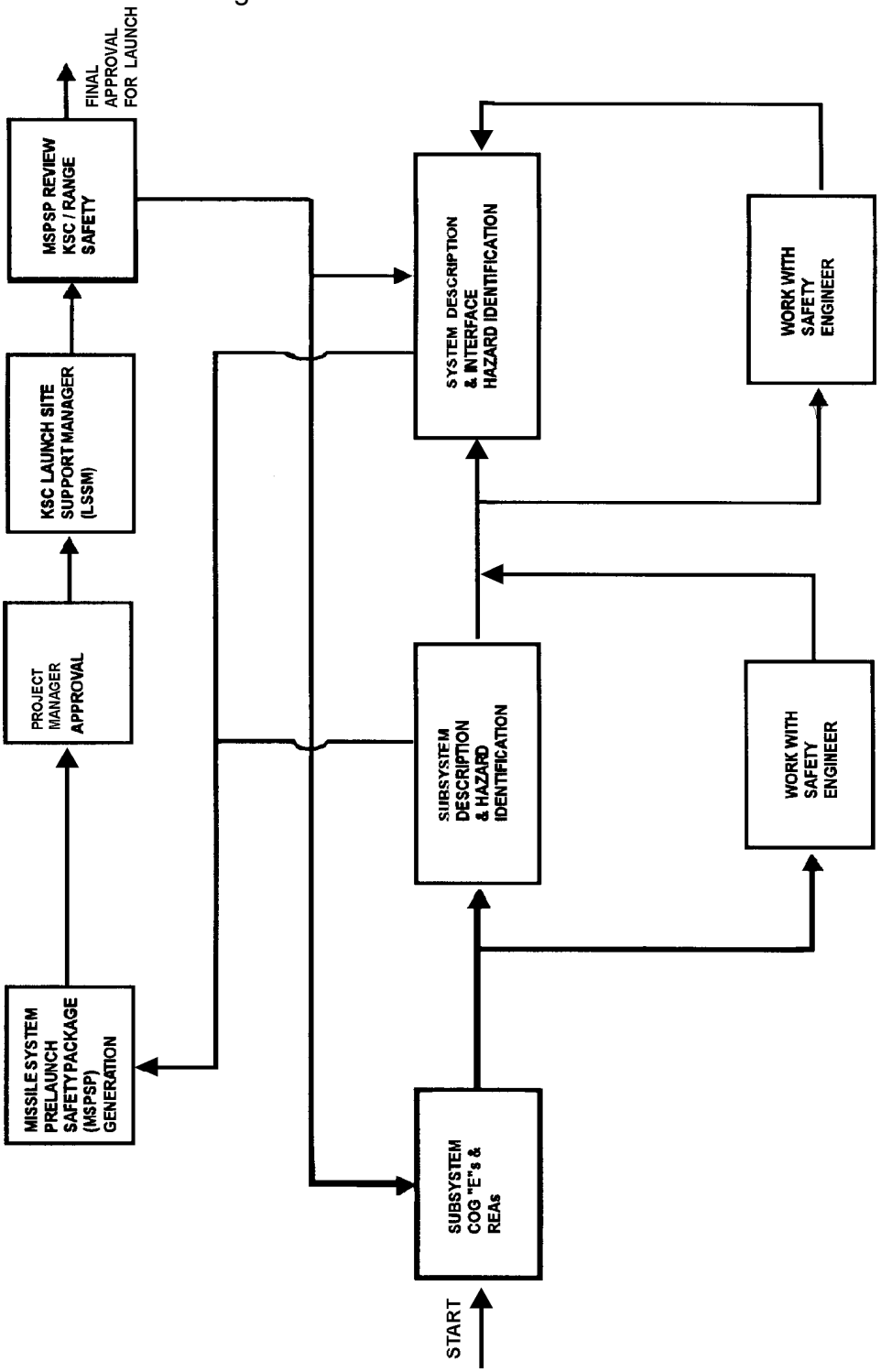
b) Payload Safety Working Group

The overall goal of the Payload Safety Working Group (PSWG) is to ensure that the MRO-05 mission/NASA provided intermedaite class LV is in compliance with the applicable safety requirements and that all safety risk is clearly identified, thoroughly understood and adequately mitigated.

The function of the PSWG is to consider the safety of the design and operations of the Orbiter and the mission unique design and operations of the integrated Launch Vehicle System (LVS). Jurisdiction of operations is limited to those operations undertaken at the ER, consisting of KSC and CCAS.

As appropriate, members include representatives from 45 SPW/ SESM, NASA KSC Safety, Launch Site Support Manager (LSSM), the NASA launch vehicle organization, Orbiter contractor, and MRO-05 Project. The PSWG presides over the MSPSP Reviews and unanimous approval of the members is required for final MSPSP approval. (Ref. Fig.4)

Figure 3: Orbiter MSPSP Generation



3.2 PROGRAM MILESTONES

3.2.1 SYSTEM SAFETY MILESTONES

The Contractor's Safety Engineer assures that a schedule of the necessary safety activities (e.g., meetings, reviews, report completion and Project coordination efforts) is provided. The Contractor's Safety Engineer will obtain concurrence of this schedule from his Project Manager. Figure 5 provides milestones for dissemination and review of the Safety Package. The schedule is phased to the Project milestones (see Figure 6). Figure 5 is furnished and updated for project management by the Contractor's Safety Engineer. It reflects current safety milestones as of the date of this document, but is subject to change as the project progresses.

3.2.2 Integrated System Activity Milestones

The MRO-05 Project Schedule (Figure 6) shows integrated Project milestones including design reviews, hardware delivery, operations, launch readiness reviews, etc. The schedule is subject to change.

Figure 4 ELV Payload Safety Review Process Documentation Flow

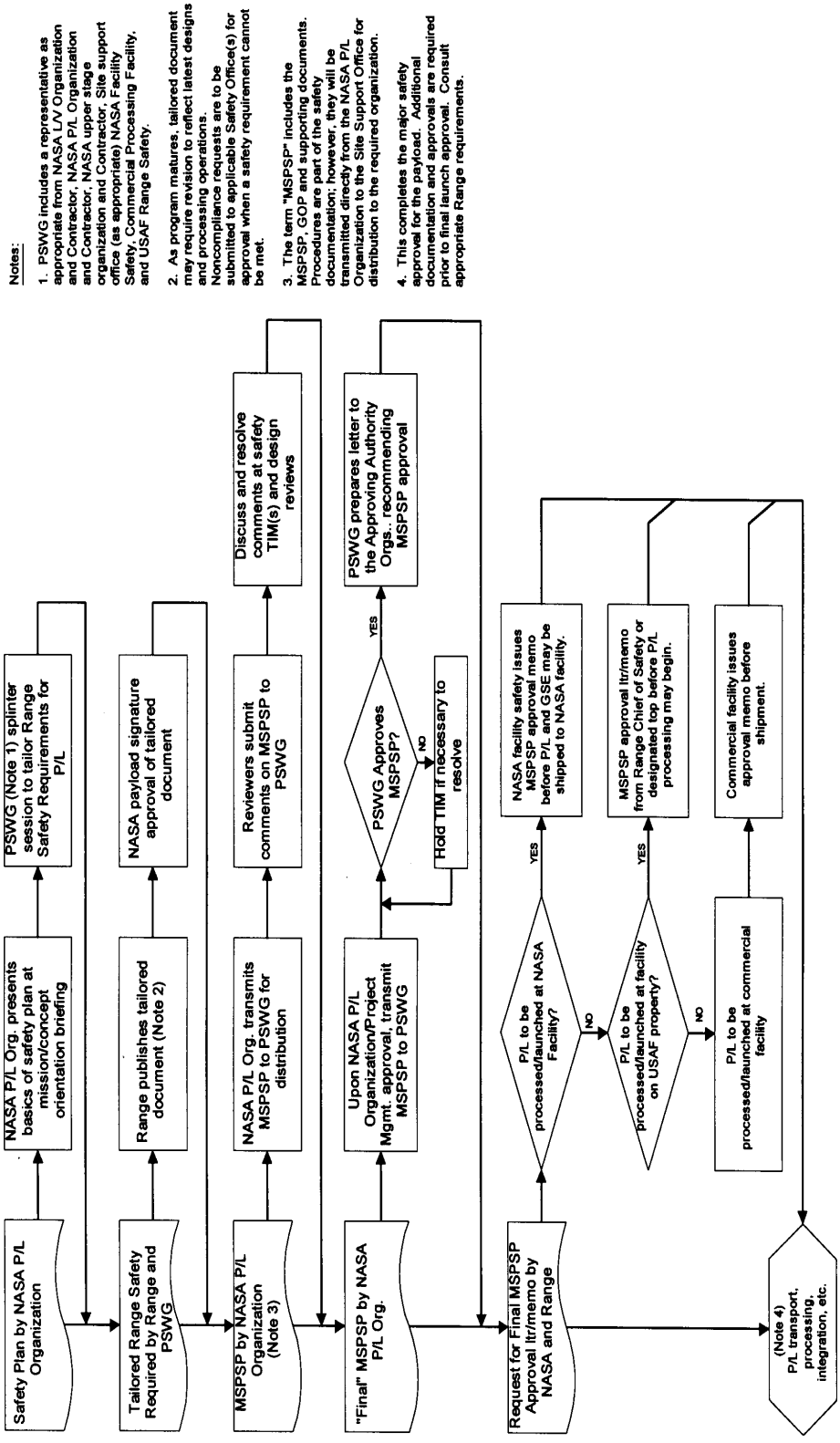


Figure 5 MRO-05 Safety Documentation Schedule

(TBD)

Fligure 6:MRO-05 Master Project Schedule

(TBD)

3.3 HAZARD CLASSIFICATION

To eliminate or control hazards, the following failure tolerance design requirements shall be satisfied:

(1) Control of catastrophic hazards
The design shall ensure that no combination of two failures or operator error can result in the death of personnel or loss of the orbiter, GSE, the launch vehicle, or other facilities or equipment.

(2) Control of critical hazards
The design shall ensure that no single failure or operator error can result in non-disabling injury of personnel or damage of the orbiter, GSE, the launch vehicle, or other facilities, equipment, and the like.

(3) Control of Design for Minimum Risk
The design of systems or subsystems including mechanisms, structural members, pressure vessels, and pressurized lines and fittings, which cannot rely on failure tolerance design mentioned above shall be controlled by applying sufficient design margins, and safety factors, selection of appropriate materials and parts, and the like, on the basis of the design concept of “Design for Minimum Risk.”

3.4 HAZARD ANALYSIS

The contractor/payload provider shall performed hazard analyses on the engineering subsystems and payload of the orbiter or GSE and the launch site operations, including interfaces among them, in order to identify all known and potential hazards arising out of or in connection with the series of operations from the delivery of the orbiter or GSE to the ER to the separation of the orbiter/GSE from the launch vehicle after lift-off.

The contractor shall start hazard analyses early in the design phase to identify hazards and reflect the analysis results in the contractor’s design, procedures, operations, and other related activities. The hazard analysis results shall be complied into a MSPS and reviewed in safety reviews as specified.

The Contractor’s Safety Engineer performs a general safety analysis of the Orbiter and support equipment to determine the initial apparent hazard level for the MRO-05 MSPSP. As the development progresses and the MSPSP is revised and updated, the Safety Engineer assesses the possible need for more detailed safety analyses (other than the standard design analysis). The Safety Engineer requests from each subsystem Cognizant Engineer (Cog E.) any new information or analysis required for complete understanding or control of any hazard. The Contractor’s Program Manager assigns action items for performing any required analysis. Examples of techniques to be considered for such safety analyses are:

- Fault Tree Analysis
- Failure Mode and Effects Analysis

- Energy Conversion Analysis
- Time Sequencing Analysis
- Sneak Circuit Analysis

System safety encompasses all activities associated with the Orbiter and GSE, whether at the contractor's facility, during transport or during the initial launch phase at the launch complex.

3.5 SAFETY DESIGN REQUIREMENTS

3.5.1 Safety design priorities are as follows:

(1) Design to eliminate, control or minimize hazards,
(2) Utilize safety equipmeHnt,
(3) Utilize protective devices,
(4) Utilize warning devices, or
(5) Apply hazard controls relying on special procedures or training

3.5.2 Control of Hazardous Functions

(1) Potentially hazardous functions which may cause a catastrophic hazard due to inadvertent operations shall be controlled by a minimum of three independent inhibits, and two out of the three inhibits shall be monitored.

(2) Potentially hazardous functions which may cause a critical hazard due to inadvertent operations shall be controlled by a minimum of two independent inhibits.

3.5.3 Radioactive Material

MRO-05 Project has edicted that no radioactive material shall be used; this includes, but is not limited to, Radioisotope Thermal-electric Generators (RTGs), and Radioisotope Heating Units (RHUs).

3.5.4 Orbital Debris

Should any part of the orbiter be intentionally released following separation from the launch vehicle, then an Orbital Debris Assessment, or the information required to produce the assessment shall be supplied in accordance with NSS 1740.14, Guidelines and Assessment Procedures for Limiting Orbital Debris.

3.6 SAFETY ASSESSMENT

Nonhazardous elements which have little complexity need only to provide review, reporting, and approval documentation necessary to assure JPL, KSC, and the 45th Space Wing (SPW) Commander/Eastern Range (ER) management of the absence of hazards. For more complicated equipment or operations, the responsible parties must provide ample assurance that safety is preserved in all areas. Since the Project safety

requirements of this plan extend to all engineering subsystems and payload, these safety activities will involve any organization that has a contract with the project.

In all areas of fabrication, development, testing, handling or operations of the engineering subsystems and payload, system safety is concerned with protection of:

- Personnel against injury or illness;
- Flight/flight-critical equipment and ground segment against damaging incidents that could result in catastrophic failures or degraded performance;
- Capital equipment and facilities.

3.6.1 Methods

The Contractor's Safety Engineer generates the MRO-05 Hazard listing as an initial activity. This package documents all hazards or potential hazards resulting from the Orbiter or associated support equipment during design, manufacture or testing. The Contractor's Safety Engineer, working with the various CogE's generates the Preliminary Hazard Analysis.

3.6.2 Risk Assessment

Decisions regarding resolution of identified hazards not meeting Safety requirements shall be based on assessment of the risk involved. These hazards shall be identified, an Exception/Waiver generated and a risk assessment attached for management approval.

Engineering Change Requests (ECRs) and waivers are reviewed for possible safety impact. The appropriate CogE is responsible for identification and control of any safety hazards that might result from a change, problem, or failure in subsystems under their cognizance.

3.6.3 Reviews

Each CogE participates, for safety evaluation purposes, in Orbiter and payload reviews associated with their particular activity. He or she also attends reviews of other subsystems that have both a sizable interface and interrelated hazard ramifications with their subsystem.

Prior to system testing of flight critical hardware in any environmental test facility, the manager of the test facility will conduct a readiness review of the facility, equipment and test plans to assure acceptable safety and readiness for the operation.

Prior to engineering subsystems or payload assembly operations at the provider's facility, or orbiter operations at the contractor, safety inspections of the facilities to be used will be performed by a small group composed of representatives from the MRO-05 Project and other personnel as deemed appropriate by the I&T Manager and the Project Safety Engineer.

Prior to the start of operations at the ER, there shall be a review of the facility and/or operational safety program and procedures. Start of operations is contingent upon a pre-operational review and approval by representatives of all involved organizations to assure compliance with safety requirements.

3.6.4 Interfaces

The JPL MRO-05 Project Manager working with the Contractor's Project Manager will resolve problems associated with determining responsibilities for any hazardous interfaces such as heat inputs to propellant tanks, etc. between the engineering subsystems, payload, or support equipment.

3.6.5 Standards for Design and Operational Requirements

Instructions to ensure safe operations are included as part of project documentation for example:

1) Design safety standards are a part of specification, review, and functional requirement documents.

2) Procedures containing hazardous operations are clearly marked in the text of the procedure where the hazardous events occur. The front covers of these procedures are marked in red "HAZARDOUS OPERATIONS."

3) Operational safety constraints are included at the proper position in procedures and are conspicuously marked.

4) Testing safety requirements and constraints are included in the applicable test plans and procedures and are conspicuously marked.

3.7SAFETY VERIFICATION

Proof shall be furnished that each feature designed to control a given hazard is in fact in place and functional. Necessary proofs are dertimined from the safety analysis, listed as “Verification Methods,” refined and occasionally redefined in the documentation review process, and reported without fail when completed. Verification consists of either test, analysis, or inspection.

3.8 SYSTEM SAFETY DATA

3.8.1 Hazard or Mishap Data

Safety data, including lessons learned from other projects, will be considered and used. A monthly "Alert/Concern Summary Report" that details current concerns shall be assessed by the Contractor’s Safety Engineer for applicable lessons learned which shall then be disseminated to the Cog Es.

3.8.2 Safety Related Data

Significant MRO-05 Project safety data shall be documented as "lessons learned" for future use in data banks or as proposed changes to applicable design handbooks and specifications by the Systems Safety Office.

3.9 FLIGHT HARDWARE PROTECTION

To assure the safety of hardware and personnel, during handling, assembly, test, transportation, and storage operations, these activities shall be done in accordance with JPL D-560 for JPL internal processing.

3.9.1 Safety Surveys

When appropriate, Facility Safety Surveys, Transportation Safety Surveys, ESD Surveys and Operations Safety Surveys shall be conducted prior to transportation or operations activities with hardware at any facility.

The Surveys shall be performed in accordance with JPL D-560 or the contractor/payload provider approved equivalent process. JPL, Contractor or payload provider shall conduct the surveys in conjunction with the agencies responsible for performing or supporting the activities. Discrepancies or outstanding issues shall be worked to the satisfaction of JPL, Contractor, or payload provieder. Surveys shall be performed sufficiently in advance of the planned activity to support correction of deficiencies without impacting the schedule.

3.10 SOFTWARE SAFETY

- Software having either of the following characteristics shall be identified as safety critical.
- Software can command a hazardous function to happen.
- Software normally prevents a hazard from occurring. Failure of the software can allow the hazard to happen.

3.10.1 Hazardous Subsystems Control

Hazards associated with each engineering subsystem or payload that are dependent upon software controls will be identified, tracked, evaluated and eliminated, or the associated risk reduced to a level acceptable to the mission through the entire life cycle of the Orbiter. Identification of hazardous subsystems dependent upon software controls will be provided in the MSPSP.

3.10.2 Approach Description

The Contractor is responsible for the safe development of hazardous software (S/W) controls for the MRO-05 Orbiter. This shall cover all aspects of software development from establishing software safety requirements through design, coding, testing and integration with hardware. The Contractor is also responsible for GSE S/W.

3.11 MISHAP REPORTING AND INVESTIGATION

The Problem/Failure Reporting and Analysis System (P/FR) or the Contractor's equivalent Anomaly Reporting System shall be used to provide a means for review of the safety aspects of reports pertaining to the flight/flight-critical subsystems or systems anomalies or problems.

Any mishap (e.g. accident, incident or close call) investigations and reporting shall be in accordance with NPG 8621.1. All others are reported through the regular communication channels and at scheduled reviews.

3.12 TRAINING AND CERTIFICATION

The Contractor (Orbiter, payload) and JPL Safety Engineer will review areas needing personnel training and certification relating to hazardous operations regardless of institution location. As a minimum, personnel will be trained and certified for activities such as crane operations involving the Orbiter or payload critical elements, propellant loading, pressure system operations, pyrotechnics handling and use, non-ionizing radiation operations, any potential where a hazardous atmosphere could result, and any other hazardous test/ operations determined by the Safety Steering Committee.

Training shall be done by organizations and personnel best qualified to do so and/or by organizations having operational responsibility. The safety engineers will assure that such requirements are met by the responsible organization.

3.13 AUDIT PROGRAM

The Orbiter Contractor, Payload Provider and JPL Safety Engineers shall periodically survey the hazardous project activities under their responsibility. Each individual is responsible for design and design changes, and its interfaces and interface changes for safety or hazardous changes. Changes in safety items or operations will be communicated to the Orbiter Manager and the Safety Engineer.

The Contractor's Safety Engineer also overviews activities associated with the Orbiter. The Contractor's Program Manager may require special safety audits of any areas, at his discretion. Formal reviews may serve as an audit if sufficient details of the hazardous activities and the safety precautions to be used are a part of the review.

Hazardous activities associated with the interface between the Orbiter and the NASA provided intermediate class launch vehicle, including orbiter preparations at the Eastern Range (KSC and CCAFS) require safety monitoring by the Project.

3.14 SYSTEM SAFETY INTERFACES

Safety engineering interfaces with all organizations including safety disciplines such as Safety Operations (personnel hazard, OSHA regulations), Environmental Affairs (environmental impact statement), Radiation Safety Committee (RF hazard), Quality Assurance and Reliability Engineering.

The Contractor's Safety Engineer interfaces with the Launch Vehicle's Safety Organization regarding interface of the MRO-05 Orbiter and the NASA provided intermediate class launch vehicle. He/she also interfaces with the Eastern Range through the KSC Launch Site Support Manger (LSSM) for all safety requirements imposed through EWR 127-1 [T] for orbiter design, ground processing and launch operations

SECTION 4

SUBMITTALS

4.1 DOCUMENTATION

This section describes those documents required to be prepared for performance of the safety tasks. A chart depicting document preparation and appropriate responsibilities is given in Figure 7. Other documentation requirements may be added as necessary.

The safety documents that will be required to assure appropriate project safety requirements are as follows:

Missile System Prelaunch Safety Package (MSPSP) is prepared to obtain Eastern Range safety approval for launching the MRO-05 Orbiter. At least two issues will be prepared by the Contractor's Safety Engineer using engineering subsystem and payload inputs.

Operating Plans and/or Procedures include test and operating plans and procedures to be used for the individual test/operation activity at the Contractor's facility, payload provider facility, JPL-operated facilities, and for ER assembly, test and launch activities. These plans and procedures contain the necessary safety restrictions and directions to assure safety requirements are met. The necessary approval of such plans and procedures will be by the Contractor's Project management and for hazardous procedures at the ER, by MRO-05 Project, and by the Air Force or KSC safety organizations.

(a) Included under this category, a Orbiter Countdown Procedure identifies hazardous operations during countdown to be included in the "Eastern Range Safety Officer's countdown." Those items involving hazards shall be clearly marked in the countdown sequence.

(b) Emergency Procedures address the types of plausible emergencies during each phase of the operations. The steps necessary to prevent injury to people and to prevent release of any hazardous material are described. Steps necessary to minimize damage to facilities and equipment are also described. The steps to be taken, the responsible people, involved emergency crews, equipment and facilities to be employed, etc., are included. The procedures will be reviewed and approved by the MRO-05 Project, Air Force and KSC Safety as appropriate.

Figure 7: Matrix of Required Safety Documentation, Responsibilities and Approvals

	PROJECT MANAGER	PROJECT SAFETY ENGINERR	ORBITER CONTRACTORS	PAYLOAD PROVIDER	COG'E	PAYLOAD SAFETY WORKING GROUP	NASA / KSC	CCAFS SAFETY	LAUNCH VEHICLE CONTRACTOR
1. MRO-05 Project Safety Plan	RS	PR	O	O	O		O	O	
2. Contractor Safety Plan	RS	RS	P	O	O				
3. Payload Provider Safety Plan	RS	RS	O	P	O				
4. Safety Waivers (external to JPL)	RS	P	P	P	RI	R	SO	SO	
5. Operating Plans/Procedures	RS	P	P			O			
6. Hazardous Procedures (at any organization including ER)		S	P	P	P	R	RS O	RS O	
7. RF Use Request/Authorization forms		R	P	I	I	R	SO	SO	
8. Missile System Pre-launch Safety Data Package	RS	RS	PS	I	I	R	RS	RS	R
9. Certificate of Safety Compliance	RS	PS	P	P					
P = Preparation Responsibilities									
R = Review Responsibilities									
S = Signature / Approval									
I = Provide Information									
O = Receive Information									
* Safety Data Package includes									
Hazard Matrices and Hazardous									
Materials Lists. Cog E's/PEM's are									
Responsible for providing Safety									
Data Package inputs.									

This page intentionally left blank

APPENDIX A

ACRONYMS

AF	Air Force
ATLO	Assembly, Test and Launch Operations
CCAFS	Cape Canaveral Air Force Station
CDR	Critical Design Review
CogE	Cognizant Engineer
ECR	Engineering Change Request
EPA	Environmental Protection Agency
ER	Eastern Range
EWR	Eastern and Western Range
GFP	Government-Furnished Property
GIDEP	Government Industry Data Exchange Program
GOP	Ground Operations Plan
GSE	Ground Support Equipment
HPWT	High Performance Work Team
HRCR	Hardware Review and Certification Record
ICD	Interface Control Document
I&T	Integration and Test
JPL	Jet Propulsion Laboratory
KSC	Kennedy Space Center
L/V	Launch Vehicle
LSSM	Launch Site Support Manager
LVS	Launch Vehicle System
MIUL	Materials Identification Usage List
MRO	Mars Reconnaissance Orbiter Project
MSPSP	Missile System Prelaunch Safety Package
NASA	National Aeronautics and Space Administration
NEPA	National Environmental Protection Act
OSHA	Occupational Health and Safety Administration
PDR	Preliminary Design Review
P/L	Payload
PFR	Problem/Failure Report
PSWG	Payload Safety Working Group

RF	Radio Frequency
SECR	Support Equipment Review and Certification Record
SDST	Small Deep Space Transponder
S/W	Software
SPW	Space Wing
SSC	Safety Steering Committee
TBD	To Be Determined
TIM	Technical Interchange Meeting
[T]	Tailored
TWT	Travelling Wave Tube
UHF	Ultra-High Frequency
USAF	United States Air Force

This page intentionally left blank.